_swissprivacy.law

La LPD refoulée en clinique : des sanctions pénales plus théoriques que pratiques

François Charlet, le 16 avril 2025

La Cour de Justice du canton de Genève a rendu un arrêt le 26 mars 2025 au sujet des dispositions pénales de la nouvelle LPD. Cet arrêt figure parmi les premiers du genre après l'entrée en vigueur de la nouvelle LPD en septembre 2023.

Arrêt ACPR/239/2025 du 26 mars 2025 de la Cour de Justice du canton de Genève

I. Résumé de l'arrêt

Cet arrêt concerne un recours formé par A contre une ordonnance de non-entrée en matière rendue par le Ministère public. La recourante avait déposé plainte contre C SA pour violation de la LPD, après avoir découvert que l'employée E de cette société avait consulté son dossier médical. La Cour de Justice rejette le recours, estimant que les conditions d'application des dispositions pénales de la LPD ne sont pas réunies, et confirme ainsi la décision du Ministère public de ne pas ouvrir d'instruction.

En l'espèce, la recourante, en apprentissage d'employée de commerce, suivait un traitement psychiatrique à la clinique F exploitée par C SA. Après avoir appris qu'une camarade de classe, E, apprentie chez C SA, avait révélé des informations médicales sur une autre apprentie, elle a demandé à vérifier qui avait consulté son propre dossier. Un relevé d'activités (logs techniques) a confirmé un accès par E le 7 juillet 2023 pendant environ 30 secondes. L'enquête a révélé que le logiciel utilisé ne permettait pas l'accès partiel à un dossier, chaque utilisateur ayant accès à l'intégralité du dossier médical informatisé.

Deux dispositions pénales de la LPD sont au cœur du litige. Premièrement, l'art. 60 al. 1 let. a LPD (obligation d'informer). La recourante estimait que C SA n'avait pas fourni d'informations complètes sur les données consultées. La Cour a jugé que la société avait respecté ses obligations en répondant dans le délai de 30 jours et dans la mesure des possibilités techniques, le logiciel ne permettant pas de savoir précisément quelles données avaient été consultées.

Secondement, l'art. 61 let. c LPD (sécurité des données). La recourante contestait le fait que

les employés administratifs puissent accéder à l'intégralité de son dossier médical. La Cour a considéré que l'accès était nécessaire pour les tâches de facturation et que la proportionnalité de cet accès relevait davantage du droit civil que du droit pénal. Seuls des cas manifestes, comme l'absence totale de mesures de protection, pourraient constituer une infraction pénale.

II. Raisonnement de la Cour

Concernant l'art. 60 LPD, la Cour estime que C SA a respecté ses obligations légales en répondant de manière complète aux questions (sic) de la recourante le 25 mars 2024, puis en précisant sa réponse le 9 avril. La Cour considère que l'information fournie était conforme aux exigences de l'art. 25 LPD. Même si la société n'a pas précisé exactement quelles données avaient été consultées le 7 juillet 2023, cette information n'était pas pertinente puisque C SA avait clairement indiqué que l'accès au dossier médical était nécessaire pour les tâches de facturation. De plus, la Cour relève que le logiciel ne permettait pas techniquement de déterminer exactement quelles données avaient été consultées, ce qui exclut toute violation intentionnelle de l'art. 60 LPD.

Concernant l'art. 61 LPD, la Cour considère que la question soulevée par la recourante relève essentiellement du droit civil et du principe de proportionnalité (art. 6 al. 2 LPD) plutôt que du droit pénal. La Cour rappelle que seuls des cas manifestes, comme l'absence totale de mesures de protection, pourraient constituer une infraction pénale sous l'angle de l'art. 61 LPD. L'existence d'un motif objectif (nécessité pour la facturation) justifiant l'accès aux dossiers médicaux et le fait que les employés administratifs soient également soumis au secret médical empêchent de considérer ce cas comme atteignant le degré de gravité requis pour une infraction pénale.

La Cour conclut qu'on peut exclure que d'éventuelles défaillances organisationnelles soient suffisamment graves pour réaliser l'infraction visée à l'art. 61 let. c LPD.

III. À retenir de ce jugement

Pour qu'une violation de l'art. 60 LPD soit établie, l'information incomplète ou inexacte doit être fournie intentionnellement. Les limitations techniques d'un système informatique excluent donc le caractère intentionnel. Ce raisonnement suggère qu'une entreprise ne peut être tenue pénalement responsable pour des informations qu'elle est techniquement incapable de fournir, ce qui établit une distinction importante entre contraintes techniques objectives et refus délibéré de communiquer des informations disponibles.

Concernant l'art. 61 LPD, seuls des cas manifestes d'absence de mesures de protection adaptées peuvent constituer une infraction pénale. En l'espèce, l'existence d'un motif objectif pour l'accès (besoins de facturation) et le fait que le personnel soit soumis au secret médical excluent une violation. De plus, la Cour note que des paramètres techniques permettaient aux médecins de restreindre la consultation d'un dossier à certains utilisateurs ou d'exclure tout accès, bien que ces options n'aient apparemment pas été utilisées pour le dossier de la recourante.

La distinction entre questions de droit civil (proportionnalité du traitement des données) et violations du droit pénal est soulignée par la Cour, qui rappelle que seules les violations graves relèvent des dispositions pénales de la LPD. Cela signifie que les personnes concernées devraient privilégier les voies civiles (comme une action en cessation du traitement illicite) plutôt que pénales pour contester la proportionnalité d'un traitement. Cette approche limite considérablement la portée des dispositions pénales de la LPD, qui sont donc réservées aux cas les plus graves.

L'arrêt met en lumière un dilemme pratique auquel sont confrontés de nombreux établissements de santé : comment concilier les besoins administratifs légitimes (facturation des actes médicaux) avec la protection des données des patients ? La Cour accepte l'argument selon lequel « l'émission des factures impliquait de connaître quelles prestations médicales avaient été fournies » et que « l'accès, par les facturistes, à l'onglet médical des dossiers était nécessaire à l'exécution de leurs tâches ». Cette position soulève des questions importantes sur la conception des systèmes d'information médicaux et les règles de sécurité qui voudraient que seules les données strictement nécessaires soient accessibles à chaque catégorie de personnel. Le jugement illustre la difficulté de mettre en pratique ces règles dans les environnements médicaux où les systèmes informatiques ne sont pas toujours conçus avec une granularité d'accès suffisante.

IV. Critiques

L'analyse de la Cour se concentre sur les aspects techniques et juridiques mais accorde moins d'attention au principe de proportionnalité, pourtant central en matière de protection des données. On pourrait soutenir que même si l'accès aux données médicales est nécessaire à des fins de facturation, un système de contrôle d'accès plus nuancé pourrait être mis en place. En effet, la mise en œuvre du principe de proportionnalité passe notamment par les mesures de sécurité qui sont décrites à l'art. 3 OPDo, lequel précise que les personnes autorisées ne doivent avoir accès « qu'aux données personnelles dont elles ont besoin pour accom-

plir leurs tâches » (al. 1 let. a). Il ne se justifie donc pas que le personnel administratif ait un accès complet au dossier médical d'une personne, sauf si cet accès est nécessaire pour ses tâches. Le fait d'être soumis au secret médical ne constitue pas à cet égard une circonstance permettant d'assouplir l'un des principes de base en matière de sécurité et de protection des données.

La Cour accepte sans grande analyse critique l'affirmation selon laquelle le personnel de facturation a besoin d'accéder à l'intégralité des dossiers médicaux, ce qui pourrait être contestable du point de vue de la protection des données dès la conception. En effet, comme je viens de l'expliquer ci-dessus, un logiciel de gestion de données doit permettre l'attribution de rôles aux différents utilisateurs, ces rôles octroyant plus ou moins de droits d'accès aux données ou aux écrans sur lesquels elles s'affichent. Le niveau de granularité offert par le logiciel doit être fin, qui plus est lorsqu'on traite des données sensibles, afin de permettre au responsable du traitement de prendre les mesures lui permettant de limiter convenablement et efficacement l'accès aux données qui ne sont pas nécessaires aux tâches de chaque membre du personnel. Il aurait été pertinent que la Cour interroge l'état de l'art en matière de systèmes d'information médicaux pour déterminer si des solutions plus respectueuses du principe de proportionnalité étaient disponibles et raisonnablement implémentables.

Le jugement établit un seuil élevé pour la responsabilité pénale en vertu des art. 60 et 61 LPD, suggérant que seules les violations intentionnelles les plus graves seraient poursuivies. Cela pourrait affaiblir l'effet dissuasif de ces dispositions alors que le Parlement fédéral a préféré des sanctions pénales au lieu de sanctions administratives et a rehaussé la limite maximale des amendes à CHF 250 000.-. Une condamnation à une amende d'un montant proportionnellement faible (p. ex. CHF 5000.-), mais une condamnation quand même, serait un message préférable à aucune condamnation. Une interprétation moins restrictive des art. 60 et 61 LPD permettrait de mieux respecter l'intention du législateur d'assurer une protection effective des données, malgré la rigueur du principe *nullum crimen, nulla poena sine lege* ancré à l'art. 1 CP.

Sur l'aspect intentionnel des infractions, la Cour n'analyse l'intention (qui couvre le dol éventuel, art. 12 al. 2 2e phrase CP) qu'en lien avec l'art. 60 LPD, et non avec l'art. 61 let. c LPD.

La Cour se fonde sur l'impossibilité technique du logiciel à préciser quelles données exactes ont été consultées pour écarter la violation intentionnelle. Cette approche est logique dans sa construction, mais ne questionne pas si cette limitation technique constitue elle-même un manquement aux obligations du responsable de traitement. On pourrait effectivement se

demander si le fait de ne pas être capable de fournir les informations détaillées sur les accès constitue une violation par dol éventuel de l'art. 61 let. c LPD. En effet, on pourrait argumenter qu'une journalisation détaillée (art. 4 OPDo) aurait dû être mise en œuvre au vu de l'absence d'une gestion plus fine des droits d'accès aux dossiers médicaux.

La question de savoir si C SA aurait pu mettre en œuvre de meilleures solutions techniques pour assurer un contrôle d'accès plus granulaire, respectant mieux le principe de proportionnalité et également celui de protection des données dès la conception, n'est pas approfondie. Or on pourrait argumenter que le responsable du traitement n'a, ici, pas pris les mesures de sécurité adéquates pour assurer cette granularité, ou n'a pas demandé au fournisseur du logiciel de le modifier afin d'offrir cette fonctionnalité. Ce comportement pourrait lui aussi être constitutif d'une violation par dol éventuel de la prescription sur les mesures minimales de sécurité.

En conclusion, cet arrêt illustre la difficulté d'appliquer les dispositions pénales de la LPD dans des situations où les défaillances organisationnelles et techniques sont présentes mais ne constituent pas des violations flagrantes. Il démontre également la nécessité pour les établissements de santé de revoir leurs systèmes d'information en tenant compte des exigences de proportionnalité et de sécurité requises par la LPD et l'OPDo, notamment en ce qui concerne la granularité des droits d'accès et la journalisation précise des consultations de données sensibles.

À l'heure où les amendes pour stationnement illicite sont plus facilement infligées que les sanctions pour violation de la LPD, on peut se demander si nos données personnelles valent moins qu'une place de parking. On retiendra enfin de cet arrêt que la granularité d'accès aux données sensibles est désormais aussi optionnelle que la lecture des conditions générales d'utilisation.

Proposition de citation : François Charlet, La LPD refoulée en clinique : des sanctions pénales plus théoriques que pratiques, 16 avril 2025 *in* www.swissprivacy.law/349